IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Stephen F. Bisbee et al.	Group Art Unit: 2137
Application No.: 10/620,817	Examiner: Zachary A. Davis
Filed: July 16, 2003	Confirmation No.: 1237
For: SYSTEM AND METHOD FOR ELECTRONIC TRANSMISSION, STORAGE AND RETRIEVAL OF AUTHENTICATED DOCUMENTS	

RESPONSE TO A RESTRICTION REQUIREMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated June 11, 2007, Applicants submit herewith a Petition for Extension of Time and the following response.

I. Election/Restrictions

In the Office Action, the Examiner sets forth a restriction requirement among two (2) groups of claims as follows:

Group I: Claims 1-18, 34 and 35, drawn to a method related to providing a Certificate Status Service; and

Group II: Claims 19-33, drawn to a method related to executing a transaction by transferring control of an authenticated information object having a verifiable evidence trail.

In response to the restriction requirement, Applicants elect Group I (corresponding to claims 1-18, 34 and 35, and drawn to a method related to providing a Certificate Status Service), with traverse.

Applicants respectfully submit that the inventions of Groups I and II should properly be examined together. As the Examiner appears to have acknowledged on page 3 of the Office Action, claim 19 refers to claim 1, and Groups I and II appear to be capable of being examined together without a serious burden on the Examiner.

Nevertheless, in order to comply with the requirements of 37 C.F.R. § 1.143, Applicants have indicated the provisional election of group I (claims 1-18, 34 and 35) for examination. Accordingly, Applicants submit that the requirements of 37 C.F.R. § 1.143 are satisfied by this response, and Applicants expressly reserve the right to file one or more divisional and/or continuation applications covering the subject matter of the non-elected claims.

II. Requirement for Information Under 37 CFR 1.105

Applicants note that in addition to the above restriction requirement, the Examiner has on page 7 and 8 of the Office Action set forth a requirement for information under 37 CFR 1.105. Specifically, on page 7 of the Office Action, the Examiner asserts "in response to this requirement, Applicant is required to provide a mark-up of the present specification showing the subject matter added or changed from the parent applications."

A. Present Specification of Serial Number 10/620,817 Marked-Up in Relation to Provisional Application Serial Number 60/397,178, filed July 18, 2002

In response to the requirement for information under 37 CFR 1.105, Applicants provide the following reply with candor and good faith under 37 CFR 1.56. A mark-up of the present specification is attached herewith showing the textual

changes between the last Provisional Application filed July 18, 2002 (Ser. No. 60/397,178) and the present utility application. For example texts deleted in the present application are shown with a strike-out, and texts that are added in the present application are shown with an underline.

B. Patent Application Serial Number 10/620,817 Summarized in Relation to The Parent Applications In The Continuation History

Wth respect to the application history as listed the domestic priority data, pertinent summary remarks are submitted below for Examiner's consideration. Applicants respectfully submit that the information being provided is in Applicants' best compliance with MPEP 704.11(a)(K); and that an effort to delineate present specification as further mark-ups would not be possible, or in the alternative, would be futile since there does not appear to be a word-for-word comparison to show the subject matter added or changed from the other applications in the continuation history. Accordingly, Applicants respectfully submit that the below summarized remarks, together with the attached specification mark-up, comprise complete Applicants' response to the Examiner's requirement for information under 37 CFR 1.105.

C. Summarized Remarks: Methods Relating to Provisional Application Serial Number 60/397,178, filed July 18, 2002

The Trusted Custodial Utility (TCU) functions as a trusted repository to control and maintain the authenticity and legal standing of each electronic original authoritative copy submitted to the TCU. Prior to introduction of the capabilities provided by the Certificate Status Service (CSS), the trusted repository was

responsible for retrieving, caching and managing the certificate status required for validating each new digital signature affixed to submitted authoritative copies. The trusted repository initially performed many of the common certificate status related functions that are now performed by the CSS.

Certificate status checking is the first of four steps necessary to validate the digital signatures of authoritative copies that help prove their authenticity. The other required steps are: second, verifying that the digital signature's message digest computes and decrypts correctly, third, checking to ensure that the digital signature was created within certificate's validity period, and fourth, checking that the identity conveyed in the authentication certificate agrees with the named party authorized to sign the electronic record. These four steps have been performed in all prior patents that relate to this Patent 7 CIP. The establishment of the CSS as a callable feature removes a significant communications and computational burden from the trusted repository and results in cleaner, more efficient and scalable architectures for both the CSS and trusted repository.

The need for a CSS became apparent early in consideration of the eOriginal™ global trade and leasing applications. The customers for these applications asked the company to simultaneously interoperate with multiple national, commercial and private Certificate Authorities (CAs). Neither trust relationships nor interoperability existed between any of these CAs. No application had succeeded at inter-working where two or more CA domains were involved. CA cross-certification efforts proved politically and technically unmanageable. Newer real-time certificate status reporting methods were also being introduced, but on an individual CA basis. Although the CSS can leverage certificate status responders

(validation authorities, OpenValidation.org, LDAP responders), their contribution is too simply to reduce CA security exposure and communication loading. The CSS addresses these challenges with capabilities introduced in the earlier patents, but resulting complexity and risk mitigation necessitated our taking a new approach in applying these and other described CSS capabilities.

Since the provisional application (Ser. No. 60/397178) filing date of July 18, 2002, Applicants have proven the viability of incorporating issuing CA domains into approved or not-approved lists for each eOriginal™ customer/subscriber organization and for each transaction type. A CA's certificates may be acceptable for a given set of subscriber transactions, while at the same time unacceptable for different set of subscribers or subscriber transactions.

The CSS acts very similar to the bank check clearing network which routes checks to the issuing bank for processing. The CSS routes certificate status requests it receives from a trusted repository to the appropriate certificate status reporting application of the certificates' issuing CA. The embodiment of CSS enforced business rules further reduces communication, computational overhead and security concerns by identifying those issuing CAs and client organizations that are approved or not approved by trusted repository subscribers. This results in a significant reduction in the number of certificates status queries otherwise required and eliminates the possibility of receiving unacceptable certificate status responses; e.g., certificate validation, but not an approved business partner or customer. These efficiencies and security techniques are not available in any prior certificate status responder patent, application or embodiment. All prior certificate responder based patents simply address whether a CA or client's certificate is valid or revoked.

The CSS organizational subscribers determine which CA's certificates are acceptable and when. The CSS design is extensible, enabling it to work with any current or future certificate status reporting protocol. This differs from prior CA certificate status responder initiatives that simply address communications and processing load balance, and that are limited to reporting certificate status for a single CA domain using a single certificate status reporting protocol.

D. Summarized Remarks In Relation to The Remaining Continuation History

Generally, much of the Patent Application Serial Number 10/620,817, as marked-up from the Provisional Application Serial Number 60/397,178, has been rewritten when compared to the other parent applications, and recounts the prior subject matters largely in the Background/Summary texts of the present application as follows:

- Page 7, line 17 through page 9, line 29 of Patent Application Serial Number 10/620,817; or
- Page 7, line 14 through page 10, line 29 of the attached marked-up specification.

The pertinent prior descriptions that support the above Background/Summary texts are variously drawn from the following issued patents in the remaining continuation history, as a whole:

- See, col. 14 line 19 – line 40; and col. 15, lines 29- 64 of US Patent 7,162,635 Issued on January 9, 2007 from Ser. No. 09/737,325;

- See, col. 9, lines 44-64; col. 11, line 20 – line 41; and col. 12, lines 30 - 65 of US 6,367,013 Issued on April 2, 2002 from Ser. No. 09/452,928;
- See, col. 15, lines 22-43, of US Patent 6,237,096 issued on May 22, 2001 from Ser. No. 09/072,079;
- See, col. 3,lines 29-36; col. 5, lines 5-27; col. 10, line 65 - col.11, line 23 of US 5,748,738 issued May 05, 1998 from Ser. No. 08/528,841; and
- See, col. 3, line 58 – col. 4, line14 of US 5,615,268 issued March 25, 1997 from Ser. No. 08/373,944.

E. As described in US 7,162,635 issued 01/09/2007 (filed 12/14/2000) and US 6,367,013 issued 04/02/2002 (filed 12/01/1999)

('013 Patent – Colum 11, line 20 – line 41)

('635 Patent - Column 14 line 19 – line 40)

FIG. 2 is a block diagram of a DAS that is in accordance with Applicants' inventions and that corresponds to FIG. 1. FIG. 2 shows the interconnections between the Certification Authority CA, which issues, revokes, renews, and publishes certificates and keeps information on certificate status, including a certificate revocation list (CRL); the Registration Authority RA, which is empowered to request and retrieve certificates; an e-original client EC, which with a user Token in the possession of a Transfer Agent, retrieves and uses certificates and CRL and certificate status information; and the Trusted Custodial Utility TCU, which is an independent, trusted third-party custodian of information objects and is the holder of its own Token(s). As indicated in FIG. 2, the CA and RA may hold their own Tokens

as well as one or more user Tokens (e.g., in connection with setup for Transfer Agent use). Although not indicated in FIG. 2, it will be appreciated that the TCU comprises at least one memory and at least one digital signal processor (DSP). Also shown in FIG. 2 is a Directory Certificate Repository DCR that stores and distributes certificates and CRLs and certificate status information. The DCR may in some embodiments be included in the Certification Authority CA.

('013 Patent – Colum 12, lines 30 - 65)

('635 Patent - Column 15, lines 29- 64)

As described above, Applicants' verifiable chain of evidence or custody can be useful for many purposes besides simply indicating the provenance or pedigree of a document or object. For example, governmental entities might use a chain of custody to help compute and collect taxes or other levies. The TCU provides such an evidence chain by receiving an original executed or signed document and verifying the identity of the signer and the authenticity of documents received. The TCU retrieves CRLs from a directory, checks the CRLs for Certificate validity, and checks the expiration date of the Certificate. In one embodiment of the inventions, the Online Certificate Status Protocol (OCSP) can be used to check certificate validity. The TCU then generates a date-time stamp for the document received, and provides an integrity block (hash) that ensures that the document cannot be altered without detection. The integrity block is protected using a digital signature algorithm, and the evidence chain uses the integrity block and date-time stamp to provide notice and evidence of any alteration, even by a document's originator, if alteration is attempted after origination.

F. As described in US 6,367,013 issued 04/02/2002 (filed 12/01/1999)

(Col. 9, Lines 44-64)

On receiving a digitally signed electronic object (block 114), the TCU tests the integrity of the electronic object's contents, the validity period of the Transfer Agent's certificate, and the status (valid or revoked) of the authentication certificate (e.g., ITU X.509v3 certificate(s)). The test of the integrity of the object contents, which may also be called "digital signature verification", comprises extracting the public key from the authentication certificate, decrypting the digital signature (thereby uncovering the object's hash), computing a new object hash, and checking the uncovered hash against the new hash. The test of the validity period comprises simply ensuring that the current date and time falls within the validity period noted in the certificate. The test of the validity of the certificate comprises querying the PKI to determine whether the certificate was not revoked or otherwise restricted at the time of digital signing. These three tests together may be called a "validation" process. Successful tests signify the authenticity of the received digitally signed electronic object, that is to say, who submitted the electronic object and that the object's contents have not changed during the submission process.

G. As described in US 6,237,096 issued 05/22/2001 (filed 05/04/1998)

(Col. 15, lines 22-43)

As described above, Applicants' invention provides for a verifiable chain of custody that can be useful for many purposes besides simply indicating the provenance or pedigree of a document or object. For example, governmental entities

might use a chain of custody to help compute and collect taxes or other levies. The TCU provides such an evidence trail by receiving an original executed or signed document and verifying the identity of the signer and the authenticity of documents received. The TCU retrieves certificate revocation lists ("CRL's") from a directory, checks the CRL for Certificate validity, and checks the expiration date of the Certificate. The TCU then generates date and time stamps for the document received, and provides an integrity block that ensures that the document cannot be altered without detection. The integrity block is provided using a digital signature algorithm to provide for non-repudiation, i.e., the ability to prove the identity of the document's originator and the identity of the authentication center. The evidence trail uses the integrity block and date and time stamps to provide notice and evidence of any alteration efforts, even by a document's originator, if alteration is attempted after origination.

H. As described in US 5,748,738 issued 05/05/1998 (filed 09/15/1995) and US 5,615,268 issued 03/25/1997 (filed 01/17/1995)

Abstract: Methods and apparatus are provided that implement digital signing and/or encryption for the electronic transmission, storage, and retrieval of authenticated documents and that enable the establishment of the identity of the originator of an electronic document and of the integrity of the information contained in such a document. Together these provide irrevocable proof of authenticity of the document. The methods and apparatus make it possible to provide "paper-less" commercial transactions, such as real-estate transactions and the financial transactions secured by real estate. A Certification Authority provides tools for

initializing and managing the cryptographic material required to sign and seal electronic documents. An Authentication Center provides "third party" verification that a document is executed and transmitted by the document's originator. The methods and apparatus eliminate the need for "hard copies" of original documents as well as hard-copy storage. Retrieval of an authenticated document from the Authentication Center may be done by any number of authorized parties at any time by on-line capability.

('738 Patent – Col. 3, Lines 29-36)

In another aspect of the invention, an apparatus for authenticating an electronic document comprises means for signing the electronic document with a digital signature of a Transfer Agent; means for appending a certificate to the electronic document; and means for validating the digital signature and certificate. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes.

('268 Patent – Col. 3, line 58 – Col 4, line14)

('738 Patent – Col. 5, Lines 5-27)

In FIG. 1, a document's originator and any subsequent transmitter are called a Transfer Agent, and it will be appreciated that a Transfer Agent is identified to the DAS by its possession of a valid public/private key and a valid PIN. In issuing the key and PIN to the Transfer Agent, the DAS advantageously records one or more characteristics of the Transfer Agent in association with the key and PIN. For

example, the Transfer Agent may be authorized to conduct only certain types of transactions and/or transactions having less than a predetermined value.

Issuance by the Certification Authority of the public/private keys permits a digitally signed certificate ensuring the identity of each transmitter of an encrypted document. The Certification Authority also retains the ability to revoke a public/private key, or to reissue a public/private key, from a remote location electronically. The Certification Authority can also provide privilege management in accordance with the policy set for the system. For example, the Certification Authority can set financial or other limits on the authority granted to the Transfer Agent based upon restrictions inserted into the certificates, such as the characteristics described above. In this way, the DAS assumes responsibility for the Certification Authority and verification of the identity of the Transfer Agent (document originator or transmitter).

('738 Patent – Col. 10, Line 65- Col.11, Line 23)

The signature validation step, which would normally, but not necessarily, be carried out by the Authentication Center, comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the

document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document.

As shown in FIG. 11, a certificate of a user (Transfer Agent) or even of a Certification Authority is preferably digitally signed in substantially the same way that electronic documents are digitally signed, except that such a certificate is signed by authorities specifically empowered to create certificates. Validation of a document's digital signatures includes validation of the public signatures of all Certification Authorities in a path between the signatory and a Root Authority, which is the most superior Certification Authority. The signatures of these Certification Authorities are loaded in the signatory's Token and appended to documents prepared with that Token.

As illustrated by FIG. 12, the path from the signatory to the Root Authority may be considered part of an authentication tree. The signatory's (user's) certificate is digitally signed by a Certification Authority whose own certificate (the CA Certificate) is signed by the Root Certification Authority. Since there is likely to be a plurality of Certification Authorities located on different branches of the authentication tree, it is only necessary to retrieve all Certification Authority certificates along both branches until a common node is encountered, in order to authenticate a digital signature for an entity on a different branch of an authentication tree, and to verify the authenticities of the certificates up to the common node.

III. Conclusion

Applicants earnestly solicit favorable consideration of the above response and early passage to issue the present application. The Examiner is invited to contact the undersigned at the below-listed telephone number, if it is believed that prosecution of this application may be assisted thereby.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: August 3, 2007 By: _____

Richard J. Kim
Registration No. 48360

Attached: mark-up of specification pursuant to 37 CFR §1.105.

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620